PRIVACY IMPACT ASSESSMENT (PIA)

For the

Advanced Skills Management (ASM)
Department of the Navy - NAVAIR

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	DITPR ID: 8396 DITPR DON ID: 21654
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI UII: 007-000002612

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier NM01500-3

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

SORN authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Commandant Marine Corps
DoD 6025.18-R Health Information Privacy Regulation
E.O. 9397 (SSN), as amended

Other authorities:

Navy directives that mandate the use of the Advanced Skills Management application are the The Naval Aviation Maintenance Program (NAMP) COMNAVAIRFORINST 4790.2 and Advanced Skills Management General Business Rules, Roles and Responsibilities, Implementation Guidance, and General Program Development Practices COMNECC Instruction 1553.1.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of ASM is to maintain records concerning training, education, and qualifications of Naval and Marine Corps military, government and contractor personnel for use by Manpower, Personnel and Training (MPT) managers.
The purpose of this system is to maintain records concerning training, education, and qualifications of Naval and Marine Corps military, government and contractor personnel for use by Manpower, Personnel and Training (MPT) managers.

ASM acts as an individual Electronic Training Jacket and Training Management system, used to assess individual training requirements and readiness, manage Naval and Marine Corps formal, general military and technical training, qualifications, certifications and licenses, and create short and long term training action plans for individuals. ASM contains master task lists and test and evaluation modules. ASM automates training administration to provide an individual record of "all things training and education" for active duty, reserve and civilian personnel. At the unit level, ASM allows for the evaluation/assessment of assigned personnel training requirements and readiness, automates unit training readiness assessments, and a determination of unit readiness percentage.

Personal information collected in ASM includes: Name, SSN (full and truncated), driver's license, DoD ID number, gender, race/ethnicity, birth date, personal cell phone number, home telephone number, personal email address, mailing/home address, spouse and child information: Name; medical information: medical/ physical exam results, blood type, and medical readiness status (cleared or not cleared); military records, and training tests and scores.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Risks associated with ASM PII include loss or theft, unauthorized disclosure.

Measures to protect High Impact PII include encryption, Common Access Card (CAC) use, password protection, PII training, and use of signature confirmation when removed from protected workplaces.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Aviation maintenance community within DoN and USMC.

☒ **Other DoD Components.**

Specify. Defense Logistics Agency

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. NAVSEA Division Keyport contractors who sign a Non Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information including PII.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

ASM does not collect PII directly from the individual.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

ASM does not collect PII directly from the individual.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.	ASM does not collect PII directly from the individual. However, the individual is able to correct erroneous information resident with in ASM. Each time a user logs into ASM they must acknowledge a Privacy Act Statement that they are accessing a system that contain PII, and its conditions of disclosure and the Standard Manadatory DoD Notice and Consent Banner regarding access to a DoD Information System.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.